Amendments to the Claims

The listing of claims below will replace all prior versions and listings of claims in this application.

Listing of Claims:

1. (Currently Amended) A method comprising:

obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;

obtaining a clear form external ~~an~~ integrity hash of first data comprising said clear form rights information and an external key as an integrity secret ~~stored in a clear form at a client device, said rights information being associated with content stored at the client device~~;

obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key;

encrypting ~~the~~ said internal integrity hash using ~~a~~ said externally inaccessible client device key ~~to generate an encrypted hash, said client device key being externally inaccessible from the client device~~; and

storing the encrypted internal integrity hash on the client device.

2. (Currently Amended) The method of claim 1 wherein obtaining the clear form external integrity hash comprises:

receiving the clear form external integrity hash from a server device.

3. (Currently Amended) The method of claim 1 wherein obtaining the internal integrity hash comprises:

generating the internal integrity hash on the client device.

4. (Currently Amended) The method of claim 1 further comprising storing said clear form external integrity hash on the client device. ~~The method of claim 3 wherein generating the integrity hash on the client device comprises:~~

~~applying the client device key in a combination with the rights information; and~~

~~determining the integrity hash from the combination of the rights information and the client device key.~~

5. (Currently Amended) The method of claim 1 further comprising receiving the external key at the client device. ~~wherein the integrity hash comprises a first integrity hash, the method further comprising:~~

~~obtaining a second integrity hash of the rights information; and~~

~~storing the second integrity hash on the client device in a clear form~~.

6. (Currently Amended) The method of ~~claim 5~~ claim 2 wherein said external key comprises a server device key. ~~obtaining the second integrity hash comprises:~~

~~receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.~~

7. (Canceled) ~~The method of claim 5 wherein obtaining the first integrity hash comprises:~~

~~applying the client device key in a combination with the rights information and the second integrity hash; and~~

~~determining the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.~~

8. (Original) The method of claim 1 further comprising:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

9. (Currently Amended) The method of claim 1 further comprising:

generating a validation hash from at least the clear form rights information;

decrypting the encrypted internal integrity hash to recover the internal integrity hash; and

comparing the validation hash to the internal integrity hash to detect tampering with the rights information.

10. (Original) The method of claim 9 further comprising:

disabling the content on the client device if tampering is detected.

11. (Currently Amended) The method of claim 1 further comprising:

storing the clear form rights information on the client device ~~in a clear form~~.

12. (Currently Amended) The method of claim 10 further comprising:

reading the clear form rights information from the client device ~~in the clear form out~~ to a server device.

13. (Currently Amended) The method of claim 1 wherein the clear form rights information ~~comprise~~ comprises usage information, the method further comprising:

tracking usage of the content;

updating the clear form rights information with changes in usage; and

for each update of the clear form rights information:

re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key; and

~~regenerating,~~ re-encrypting, and ~~restoring~~ re-storing the internal integrity hash on the client device ~~for each update of the rights information~~.

14. (Currently Amended) The method of claim 1 wherein the internal integrity hash comprises a Hash Message Authentication Code (HMAC).

15. (Original) The method of claim 1 wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path.

16. (Original) The method of claim 1 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

17. (Currently Amended) The method of claim 1 further comprising at least one of:

downloading the clear form rights information from a server device; and

installing a storage medium having the clear form rights information stored thereon.

18. (Currently Amended) The method of claim 1 wherein the clear form rights information ~~grant~~ grants unlimited play for the content on the client device.

19. (Original) The method of claim 3 wherein generating the internal integrity hash comprises generating the internal integrity hash in trusted hardware.

20-30. (Canceled)

31. (Currently Amended) A method comprising:

generating a validation hash from ~~at least~~ validation data comprising stored clear form rights information associated with content stored on a client device;

decrypting an encrypted hash to recover an integrity hash using an externally inaccessible client device key ~~that is externally inaccessible from the client device~~, said integrity hash having been previously generated from ~~at least~~ data comprising the stored clear form rights information ~~associated with the content~~ and a clear form hash of at least the clear form rights information; and

comparing the validation hash to the integrity hash to detect tampering with the clear form rights information.

32. (Original) The method of claim 31 further comprising:

disabling the content on the client device if tampering is detected.

33. (Original) The method of claim 31 further comprising:

receiving a usage request for the content stored at the client device, said usage request to initiate generation of the validation hash and comparison to the integrity hash; and

permitting usage only if the content is not disabled.

34. (Currently Amended) A client device comprising:

a register operative to store a client device key, said register being externally inaccessible from the client device;

a memory operative to store content and clear form rights information associated with the content, said memory being externally accessible;

hash circuitry operative to:

obtain ~~an~~ a clear form external integrity hash of first data comprising the clear form rights information and an external key as an integrity secret; and

obtain an internal integrity hash of second data comprising the clear form rights information, the clear form external integrity hash, and the externally inaccessible client device key; and

encryption circuitry operative to encrypt the internal integrity hash using the client device key ~~to generate an encrypted hash~~;

said memory being further operative to store the encrypted hash.

35. (Currently Amended) The client device of claim 34 wherein the hash circuitry is operative to obtain the clear form external integrity hash from a server device.

36. (Currently Amended) The client device of claim 34 wherein the hash circuitry is operative to generate the internal integrity hash on the client device.

37. (Canceled) ~~The client device of claim 36 wherein, to generate the integrity hash, the hash circuitry is to apply the client device key in a combination with the rights information, and to determine the integrity hash from the combination of the rights information and the client device key~~.

38. (Currently Amended) The client device of claim 34 ~~wherein the integrity hash comprises a first integrity hash, the hash circuitry further to obtain a second integrity hash of the rights information~~, said memory being further operative to store the ~~second~~ clear form external integrity hash ~~in a clear form~~.

39. (Currently Amended) The client device of ~~claim 38~~ claim 35 wherein the external key comprises a server device key. ~~, to obtain the second integrity hash, the hash circuitry is to receive the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key~~.

40. (Canceled)

41. (Currently Amended) The client device of claim 34 wherein the encryption circuitry is further operative to encrypt a content key for the content using the client device key ~~to generate an encrypted content key~~; and the memory is further operative to store the encrypted content key on the client device.

42. (Currently Amended) The client device of claim 34 wherein

the hash circuitry is operative to generate a validation hash from at least the clear form rights information; and

the encryption circuitry is further operative to decrypt the encrypted hash to recover the internal integrity hash;

the client device further comprising:

a comparator to compare the validation hash to the internal integrity hash to detect tampering with the clear form rights information.

43. (Original) The client device of claim 42 further comprising:

a content controller to disable the content on the client device if tampering is detected.

44. (Canceled)

45. (Currently Amended) The client device of claim 34 wherein the rights information ~~comprise~~ comprises usage information, the client device further comprising:

tracking circuitry to track usage of the content and update the clear form rights information with changes in usage;

wherein the hash circuitry and the encryption circuitry are further operative to regenerate, re-encrypt, and re-store the internal integrity hash in the memory for each update of the rights information.

46. (Original) The client device of claim 34 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

47. (Currently Amended) The client device of claim 34 further comprising at least one of:

an input port to download the clear form rights information from a server device; and

a storage medium port to receive a storage medium having the clear form rights information stored thereon.

48. (Original) The client device of claim 47 wherein the memory at least partially comprises the storage medium.

49. (Currently Amended) A machine readable medium having stored thereon machine executable instructions, the execution of which to implement a method comprising:

receiving clear form rights information at a client device, said rights information being associated with content stored on the client device, said client device having a client device key that is externally inaccessible from the client device;

storing the clear form rights information on the client device ~~in a clear form~~;

obtaining ~~an~~ a clear form external integrity hash of first data comprising the clear form rights information and an external key as an integrity secret;

obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key;

encrypting the internal integrity hash using the externally inaccessible client device key ~~to generate an encrypted hash~~; and

storing the encrypted internal integrity hash on the client device.

50. (Currently Amended) The machine readable medium of claim 49 wherein obtaining the integrity hash comprises:

receiving the clear form external integrity hash from a server device.

51. (Currently Amended) The machine readable medium of claim 49 wherein obtaining the internal integrity hash comprises: generating the internal integrity hash on the client device.

52. (Currently Amended) The machine readable medium of claim 49 further comprising storing said clear form external integrity hash on the client device. ~~The machine readable medium of claim 49 wherein generating the integrity hash on the client device comprises:~~

~~applying the client device key in a combination with the rights information; and~~

~~determining the integrity hash from the combination of the rights information and the client device key.~~

53. (Canceled)

54. (Currently Amended) The machine readable medium of claim 50 ~~53~~ wherein said external key comprises a server device key ~~obtaining the second integrity hash comprises:~~

~~receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key~~.

55. (Canceled)

56. (Original) The machine readable medium of claim 49 wherein the method further comprises:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

57. (Currently Amended) The machine readable medium of claim 49 wherein the method further comprises:

generating a validation hash from at least the clear form rights information;

decrypting the encrypted internal integrity hash to recover the internal integrity hash; and

comparing the validation hash to the internal integrity hash to detect tampering with the clear form rights information.

58. (Original) The machine readable medium of claim 57 wherein the method further comprises:

disabling the content on the client device if tampering is detected.

59. (Currently Amended) The machine readable medium of claim 49 wherein the clear form rights information grants unlimited play for the content on the client device.

60. (Currently Amended) The machine readable medium of claim 59 wherein the method further comprises:

reading the clear form rights information from the client device ~~in the clear form~~ out to a server device.

61. (Currently Amended) The machine readable medium of claim 49 wherein the clear form rights information comprises usage information, the method further comprising:

tracking usage of the content;

updating the clear form rights information with changes in usage; and

for each update of the clear form rights information:

re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key; and

~~regenerating,~~ re-encrypting, and ~~restoring~~ re-storing the internal integrity hash on the client device ~~for each update of the rights information~~.